2011 - Nominet consultation on domain names used in connection with criminal activity

This response is structured around the questions in Nominet's consultation paper [1]:

1. Should Nominet have an abuse policy and would creation of one be in line with its vision of making the internet a trusted space? [section1, and section 2(a)]

Yes. The creation of an abuse policy would increase confidence both that domains will not be suspended without good reason and that the use of domains for criminal purposes can be dealt with. A policy created and promoted by Nominet will help .uk registrars to behave consistently, thus strengthening the reputation of the TLD.

2. Should the issue of criminal conduct by domain name holders only be dealt with through registrars and hosts, and/or strengthening the 'due diligence' obligations of Nominet's registrars? Would there be benefits in sharing information with registrars as is currently done with the phishing feed? [section 2(a)]

Hosts, registrants and registrars are the best place to address criminal behaviour on the network. These are likely to have the best understanding of the circumstances and the most proportionate remedy. They are also likely to have tools not available to Nominet as registry. For example if a legitimate website has been compromised and is also being used for criminal purposes, suspending the domain is likely to involve disproportionate damage.

Nominet should only act against a domain if the host, registrant and registrar are unable or unwilling to help – for example if it appears that a domain has been registered solely for a criminal enterprise when the registrar may themselves be a suspect. Nominet might, however, offer to act as a conduit for passing information to registrars if it can do this more efficiently than law enforcement authorities.

3. Which types of activity would an abuse policy seek to discourage? [section 2(c)]

The creation of a Nominet abuse policy, by indicating that criminal activity on UK domains will be dealt with effectively, should aim to discourage criminals from registering domains within .uk for their activity. The policy should not attempt to cover the criminal use of legitimate domains, for example as a result of compromise of hosts or misuse of legitimate services, since this is much better dealt with by those who operate services, computers and (to some extent) networks.

4. In what circumstances would suspension of a website be proportionate? [section 2(a) para 8 & 13, section 2(f) para 31] Would there need to be an ascertained level of harm or criminality? [section 2(c), paras 21-22]

Note, first, that Nominet cannot suspend "a website", it can only suspend a delegated domain,

which will have the effect of stopping all use of that domain and its subdomains. For example if a domain used by a company (e.g. nominet.org.uk) is suspended, that company will be unable to send or receive e-mail; it will be unable to offer any other Internet services; it may have difficulty accessing Internet services provided by others; and its internal IT systems may well be disrupted. Many domains host multiple websites and services operated by different and unconnected organisations. Applying a sanction that will effectively disconnect all of these must therefore be done extremely carefully.

The proportionality of suspending a domain must therefore balance:

(a) The harm that may be caused if the domain is not suspended (for example by the continuation of criminal activity), against
(b) The harm that may be caused if the domain is suspended (for example by interrupting the legitimate business of those using the domain and their customers).

Since it will often be hard to assess the harm that will be caused by suspension (b) because it will not be practical to determine all the uses of the domain, it seems unlikely that this will clearly be outweighed by any harmful activity (a) that does not reach at least the threshold of criminality. Even then, if there is significant legitimate use of the domain, suspension is still likely to be disproportionate, suggesting that the threshold of “serious crime” may be a better measure.

As discussed in question 2, action should be taken as close to the problem as possible so Nominet should only act to suspend a domain if the host, registrant and registrar are unwilling or unable to deal with the problem.

Where there is doubt about proportionality, it may be better to have the issues assessed by a court. The paper indicates that such a process already exists and is used for civil wrongs. It is not clear whether there is an equivalent court process that could order the suspension of domains used for crimes.

5. How can Nominet avoid the risk of legal liability, when asked to take action against offences which are challenging for assessments of criminality, such as certain alleged speech offences? [section 2 (c), para 19]

Nominet is perhaps the organisation least able to take proportionate action against on-line criminality, since the only action available to it is to suspend an entire domain, with the extensive side-effects described in section 4 above. It is therefore troubling if it can be compelled by potential criminal liability to implement such a broad sanction without any assessment of whether the consequences are proportionate to the threat. Could Nominet be required, for example, to suspend the domain of a social network site or newspaper if they were notified that one comment (perhaps not even made by a member of the site) was alleged to glorify terrorism? The correct organisation to deal with such problems is the operator of the site, not the registry.

6. Should a list of offences, over which Nominet will take action, be created? [section 2(c), paras 21-22]

No. An exhaustive list of offences will need continuous updating, as new crimes are created or the severity of existing crimes changed. It would be better to use a threshold that already exists within the legal system, for example the definition of “serious crime” or another measure

based on maximum sentence.

7. Would suspensions be limited to breaches of domestic criminal law, or apply to all countries or those where the registrant expects his activities to have effect? [section 2(d)]

For practical reasons, suspensions should be limited to activities that would be a breach of domestic criminal law if targeted at UK consumers. As the paper points out, Nominet will otherwise need to be able to assess the laws of all jurisdictions on the Internet. There would also be a risk of applying different legal standards from outside the UK to the .uk domain.

The paper suggests that such an approach might create a safe haven for "rogue pharmacists" in the .uk domain – however we had understood that UK law on the sale of pharmaceutical products (which would be the standard applied under this proposal) was comparatively strict for example the *Medicines (Advertising) Regulations 1994* [2].

8. What standard of evidence might be required, and who would assess it (eg SPoC and/or Nominet) [section 2(f), para 31-32]

On the principle that evidence should be assessed by those most capable of doing so, evidence of criminality should be assessed by a SPoC alongside an initial assessment of impact and therefore proportionality. Nominet, with their greater knowledge of DNS, should then verify the assessment of impact (including, so far as possible, who will be affected and in what way) and inform the SPoC if any change to that assessment alters the question of proportionality.

However this may require a change to the legal liability position if, as suggested in question 5 and paragraph 19, the initial notification from the SPoC could immediately fix Nominet with potential legal liability. This would make it hard for them to reach a different decision on proportionality from the SPoC's initial assessment, thereby removing important information from the proportionality assessment.

9. Would a formal relationship be necessary to accept instruction? Who would be able to request suspensions? [section 2(f), para 33)

10. What principles should govern the form of an acceptable request? Should a formalised standard operating procedure and data sharing arrangement be created between Nominet and law enforcement? [section 2(f), para 34-36]

Yes, to both questions. Accidental or malicious suspension of a domain could be highly disruptive to a legitimate business, and any process leading to it must therefore be well protected. The consequences of error or misuse appear at least as serious as those when disclosing communications data under section 22 [3] of the *Regulation of Investigatory Powers Act 2000*. That section is supported by a register of those who have been trained to make requests for disclosure; there are also standard processes [4] for authorising and making requests and for recipients to verify the identities of those making them. Equivalent training, authorisation and processes should be established for domain suspensions.

11. If suspension does occur, is there a post-suspension continuing obligation to prevent [non-]criminal conduct when the registrant uses the same registration details? [section 2(g), para 37]

If such a duty exists or is established it would create an onerous duty for registrars and registries, effectively requiring the registry to scrutinise all applications for domains and then monitor their subsequent use in case this appears to be criminal (note that placing such a duty on an ISP would be prohibited by the *eCommerce Directive*). In practice this could easily degenerate into a ban on any registration using registration details that have been the subject of a suspension request. If, as the paper suggests, criminals are in any case using incorrect registration details this will create no hindrance to them, while having the potential to create disastrous consequences for a genuine registrant whose domain is accused of involvement in criminal activity.

12. Would there need to be any form of appeals process? [section 2(b) para 16)

Yes. The consequences of any unjustified suspension of a domain, both for the registrant and for the reputation of the .uk TLD, would be very serious. An appeals process (even if, as we hope, it is very seldom used) is essential to maintaining confidence in the TLD.

13. Are there other regulatory or self-regulatory frameworks that would provide useful background or experiences? [see eg footnotes 35 & 40 & 74]

As in the response to question 10, the communications data access regime under the *Regulation of Investigatory Powers Act 2000* provides a useful comparison for the measures required to protect a process with less serious consequences if misused. It is also worth noting that the Internet Watch Foundation, though dealing with some of the most serious criminal content on-line, prohibits its members from blocking at the DNS domain level because of the potentially serious consequences of doing so.

Links
[1] http://www.nominet.org.uk/news/latest/?contentId=8274
[2] http://www.legislation.gov.uk/uksi/1994/1932/contents/made
[3] http://www.legislation.gov.uk/ukpga/2000/23/section/22
[4] http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-acquisition